Test scenario	Perform the following checks for each "Biometric Template": 1) Search for the Biometric Data Block (Tag '7F2E') inside the Biometric Template. 2) If Tag '7F2E' is present, analyze the encoding of the bytes that follow the Biometric Data Block tag. 3) If Tag '7F2E' is present, verify the length of the Enciphered Biometric Data Block DO. 4) If Tag '7F2E' is present, verify that the tag for the Biometric Data Block (Tag '5F2E') is absent. 5) If Tag '7F2E' is absent, verify that the tag for the Biometric Data Block (Tag '5F2E') is present.
Expected results	1) Tag '7F2E' may be present and shall not occur more than once. 2) If Tag '7F2E' is present, the bytes that follow the Biometric Data Block Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3) If Tag '7F2E' is present, the encoded length shall match the size of the Biometric Data Block DO. 4) If Tag '7F2E' is present, Tag '5F2E' shall be absent. 5) If Tag '7F2E' is absent, Tag '5F2E' shall be present.

A.3.10.20 Test case SE_LDS_DG9_020

Test case-ID	SE_LDS_DG9_020
Purpose	This test checks the encoding of the BIR payload (Tag '53') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:—, Annex C
Profile	DG9
Preconditions	1) EF.DG9 has been retrieved from the IDL. 2) The Biometric Group Template has been retrieved from EF.DG9.
Test scenario	Perform the following checks for each "Biometric Template": 1) Search for the BIR payload (Tag '53') inside the Biometric Template. 2) If Tag '53' is present, analyze the encoding of the bytes that follow the BIR payload tag. 3) If Tag '53' is present, verify the length of the BIR payload DO. 4) If Tag '53' is present, verify that the tag '73' is absent.
Expected results	1) Tag '53' may be present and shall not occur more than once. 2) If Tag '53' is present, the bytes that follow the BIR payload Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3) If Tag '53' is present, the encoded length shall match the size of the BIR payload DO. 4) If Tag '53' is present, Tag '73' shall be absent.

A.3.10.21 Test case SE_LDS_DG9_021

Test case-ID	SE_LDS_DG9_021
Purpose	This test checks the encoding of the BIR payload (Tag '73') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:—, Annex C
Profile	DG9
Preconditions	1) EF.DG9 has been retrieved from the IDL. 2) The Biometric Group Template has been retrieved from EF.DG9.
Test scenario	Perform the following checks for each "Biometric Template": 1) Search for the BIR payload (Tag '73') inside the Biometric Template. 2) If Tag '73' is present, analyze the encoding of the bytes that follow the BIR payload tag. 3) If Tag '73' is present, verify the length of the BIR payload DO. 4) If Tag '73' is present, verify that the tag '53' is absent.
Expected results	1) Tag '73' may be present and shall not occur more than once. 2) If Tag '73' is present, the bytes that follow the BIR payload Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3) If Tag '73' is present, the encoded length shall match the size of the BIR payload DO. 4) If Tag '73' is present, Tag '53' shall be absent.

A.3.10.22 Test case SE_LDS_DG9_022

Test case-ID	SE_LDS_DG9_022
Purpose	This test checks the encoding of the Security Block (Tag '5F3D') (if present) in each "Biometric Template" in the "Biometric Group Template" in EF.DG9.
Version	1.0
References	ISO/IEC 18013-2:—, Annex C
Profile	DG9
Preconditions	1) EF.DG9 has been retrieved from the IDL. 2) The Biometric Group Template has been retrieved from EF.DG9.
Test scenario	Perform the following checks for each "Biometric Template": 1) Search for the Security Block (Tag '5F3D') inside the Biometric Template. 2) If Tag '5F3D' is present, analyze the encoding of the bytes that follow the Security Block tag. 3) If Tag '5F3D' is present, verify the length of the Security Block DO.

Expected results	1) Tag '5F3D' may be present and shall not occur more than once. 2) If Tag '5F3D' is present, the bytes that follow the Security Block Tag shall contain a valid length encoding (according to ASN.1 encoding rules). 3) If Tag '5F3D' is present, the encoded length shall match the size of the Security Block DO.

A.3.11 Test unit SE_LDS_SOD — Tests for EF.SOD

A.3.11.1 General

Test unit-ID	SE_LDS_SOD (Standard Encoding — Document Security Object)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Security Object.
References	ISO/IEC 18013-2 ISO/IEC 18013-3

A.3.11.2 Test case SE_LDS_SOD_001

Test case-ID	SE_LDS_SOD_001
Purpose	This test checks the template tag; the encoded EF.SOD element starts with.
Version	1.0
References	ISO/IEC 18013-3
Profile	PA
Preconditions	1) EF.SOD has been retrieved from the IDL.
Test scenario	1) Check the very first byte of the EF.SOD element.
Expected results	1) The first byte shall be '77'.

A.3.11.3 Test case SE_LDS_SOD_002

Test case-ID	SE_LDS_SOD_002
Purpose	This test checks the encoding of EF.SOD element length.
Version	1.0
References	ISO/IEC 18013-3
Profile	PA
Preconditions	1) EF.SOD has been retrieved from the IDL.
Test scenario	1) Analyze the encoding of the bytes that follow the template tag. 2) Verify the length of the EF.SOD object.
Expected results	1) The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2) The encoded length shall match the size of the given EF.SOD object.

A.3.11.4 Test case SE_LDS_SOD_003

Test case-ID	SE_LDS_SOD_003
Purpose	This test checks the ASN#1 encoding of the PCKS#7 signedData object.

Version	1.0
References	ISO/IEC 18013-3 RFC-3369
Profile	PA
Preconditions	1) EF.SOD has been retrieved from the IDL.
Test scenario	1) Analyze the ASN.1 encoding of the content of EF.SOD. 2) Analyze the value of the EF.SOD template.
Expected results	1) The signedData object shall be DER encoded. 2) The value of the EF.SOD template shall be a ContentInfo data element of the SignedData Type as specified in RFC-3369.

A.3.11.5 Test case SE_LDS_SOD_004

Test case-ID	SE_LDS_SOD_004
Purpose	This test checks the value encoded in the signedData element.
Version	1.0
References	ISO/IEC 18013-3 RFC-3369
Profile	PA
Preconditions	1) EF.SOD has been retrieved from the IDL. 2) The SignedData field has been retrieved from the ContentInfo DO in EF.SOD.
Test scenario	1) Check the SignedData version value (Tag '02'). 2) Check the digestAlgorithms list (Tag '31'). 3) Check the eContentType (Tag '06'). 4) Check the certificates list (Tag 'A0'). 5) Check the Certificate Revocation Lists (Tag 'A1').
Expected results	1) The version shall be 3. 2) The digestAlgorithms list may contain all used digestAlgorithms in the signedData. The digestAlgorithms list shall not contain other digest algorithms than those specified in ISO/IEC 18013-3:2017, 8.1.4. 3) The eContentType shall have OID as specified in ISO/IEC 18013-3:2017, Table 2. 4) Tag 'A0' may be present and shall occur only once. 5) Tag 'A1' shall be absent.

A.3.11.6 Test case SE_LDS_SOD_005

Test case-ID	SE_LDS_SOD_005
Purpose	This test checks the SignerInfo element of the signedData structure.
Version	1.0
References	ISO/IEC 18013-3 RFC-3369

Profile	PA
Preconditions	1) EF.SOD has been retrieved from the IDL. 2) The SignedData field has been retrieved from the ContentInfo DO in EF.SOD.
Test scenario	Perform the following checks for each entry of the "signerInfos" field in the signedData structure: 1) Check the signer info version (Tag '02'). 2) Check the choice in the sid field (first instance of Tag '30'). 3) Check the certificate identified in the sid field. 4) Check the digestAlgorithm field (second instance of Tag '30'). 5) Check the presence of the Digest Algorithm Identifier in the digestAlgorithmlist of the signedData element. 6) Check the signedAttrs element (Tag 'A0'). 7) Check the value of the signedAttrs element. 8) Check the value of the signedAttrs element. 9) Check the message-digest Attribute. 10) Check the content-type Attribute. 11) Check the SigningTime attribute if present. 12) Check the signatureAlgorithm element. 13) Check the signature element.

Expected results	1) The version shall be 1 or 3. 2) The sid field shall match the signer info version value (version 1 if issuerandSerialNumber is used and 3 if subjectKeyIdentifier is used). 3) The certificate identified in the sid field shall be included in the signed data certificates list or available from a trusted source. 4) The digestAlgorithms list shall be one of the algorithms specified in ISO/IEC 18013-3:2017, 8.1.4 (i.e. only the following algorithms are allowed: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512). 5) The digestAlgorithm should be included in the digestAlgorithmlist of the signedData element. 6) Tag 'A0' shall be present and shall occur only once. 7) The signed attributes list shall contain the message-digest attribute. 8) The signed attributes list shall contain the content-type attribute. 9) The value of the message-digest attribute shall match the hash value of the eContent element (using the digestAlgorithm specified above). 10) The content-type attribute value shall match the encapContentInfo eContentType value in the signed-data. 11) The signing time shall be within the validity period of the signing certificate. 12) The signature algorithm shall refer to an algorithm specified in ISO/IEC 18013-3:2017, 8.1.5 [i.e. the algorithm shall be using RSASSA-PSS, RSASSA-PKCS1-v1.5, or ECDSA (ANSI X9.62)]. 13) The signature shall be valid.

A.3.11.7 Test case SE_LDS_SOD_006

Test case-ID	SE_LDS_SOD_006
Purpose	This test checks the LDS Security Object stored as eContent in the signedData Object.
Version	1.0
References	ISO/IEC 18013-3 RFC-3369
Profile	PA
Preconditions	1) EF.SOD has been retrieved from the IDL. 2) The SignedData field has been retrieved from the ContentInfo DO in EF.SOD.

Test scenario	1) Check the ASN.1 encoding of the LDS Security Object. 2) Check the encoding of the LDS Security Object. 3) Check the LDS Security Object version (Tag '02'). 4) Check the digestAlgorithm identifier. 5) Check the DataGroupHash Sequence. 6) Check the dataGroup numbers in the DataGroup Hash Sequence. 7) Check the dataGroup numbers in the DataGroup Hash Sequence. 8) Check the dataGroup hash values in the Hash Sequence.
Expected results	1) The LDS Security Object shall be DER encoded. 2) The encoding of the LDS Security Object shall follow the ASN1.1 encoding specified in ISO/IEC 18013-3:2017, 8.1.5.1. 3) The version shall be 0. 4) The digestAlgorithms list shall be one of the digest algorithms specified in ISO/IEC 18013-3:2017, 8.1.4 (i.e. SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512). 5) The Hash Sequence shall contain at least the entries for DG 1. 6) The Hash Sequence shall contain a hash value for all present data groups. The Hash Sequence shall not contain additional hash value for non-existing data groups. 7) The referred data groups shall match the Data Group list in the EF.COM. 8) All hash values shall be valid.

A.3.11.8 Test case SE_LDS_SOD_007

Test case-ID	SE_LDS_SOD_007
Purpose	This test checks the signing certificate used to verify the EF.SOD object.
Version	1.0
References	ISO/IEC 18013-3 RFC-3280
Profile	PA
Preconditions	1) EF.SOD has been retrieved from the IDL. 2) The SignedData field has been retrieved from the ContentInfo DO in EF.SOD. 3) The Signing Certificate has been retrieved (from the SignedData structure or from a trusted source). 4) The Issuing Authority Certificate has been retrieved from a trusted source.

Test scenario	1) Check the ASN.1 encoding of the signing certificate. 2) Check the ASN.1 structure of the signing certificate. 3) Check the signing certificate version. 4) Check the signature field of the certificate. 5) Check the certificates validity period. 6) Check the certificates issuer element. 7) Check the subjectPublicKeyInfo element. 8) Check the AKID extension in the signing certificate. 9) Check that the SubjectKeyIdentifier extension of the country signing certificate matches the AuthorityKeyIdentifier of the signing certificate. 10) Check the keyUsage extension of the signing certificate. 11) Check the signatureAlgorithm element. 12) Verify the signatureValue of the signing certificate with the public key of the Issuing Authority certificate.
Expected results	1) The signing certificate shall be DER encoded. 2) The signing certificate shall be encoded as specified in RFC 3280. 3) The version shall be 2. 4) The algorithm indicated in the signature element shall match the OID in the signatureAlgorithm field. 5) The validity period shall use UTC time for dates until 2049 and shall use GeneralisedTime for dates after 2049 inclusive. (NOTE It is not necessary that the certificate is still valid; it shall only have been valid at signing time). The validity period of the signing certificate shall be within the validity period of the country signing certificate. 6) The issuer shall match the subject of the provided country signing certificate. 7) The algorithm identifier in the subjectPublicKeyInfo shall refer to a algorithm specified in ISO/IEC 18013-3:2017, 8.1.5 (i.e. the algorithm shall be using RSASSA-PSS, RSASSA-PKCS1-v1.5, or ECDSA). 8) The AKID extension shall be present and shall contain a keyIdentifier value. 9) The SubjectKeyIdentifier extension shall match the AKID of the signing certificate. 10) The keyUsage extension shall be marked critical and only the digitalSignature bit shall be set. 11) The signatureAlgorithm shall indicate one of the algorithms specified in ISO/IEC 18013-3:2017, 8.1.5 (i.e. the algorithm shall be using RSASSA-PSS, RSASSA-PKCS1-v1.5, or ECDSA). 12) Verification shall be successful.

A.3.12 Test unit SE_LDS_DG12 — Tests for EF.DG12

A.3.12.1 General

Test unit-ID	SE_LDS_DG12 (Standard Encoding — Data Group 12)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Data Group 12.
References	ISO/IEC 18013-2 ISO/IEC 18013-3

A.3.12.2 Test case SE_LDS_DG12_001

Test case-ID	SE_LDS_DG12_001
Purpose	This test checks the template tag that the encoded EF.DG12 element starts with.
Version	1.0
References	ISO/IEC 18013-3
Profile	NMA
Preconditions	1) EF.DG12 has been retrieved from the IDL.
Test scenario	1) Check the very first byte of the EF.DG12 element.
Expected results	1) The first byte shall be '71'.

A.3.12.3 Test case SE_LDS_DG12_002

Test case-ID	SE_LDS_DG12_002
Purpose	This test checks the encoding of EF.DG12 element length.
Version	1.0
References	ISO/IEC 18013-3
Profile	NMA
Preconditions	1) EF.DG12 has been retrieved from the IDL.
Test scenario	1) Analyze the encoding of the bytes that follow the template tag. 2) Verify the length of the EF.DG12 object.
Expected results	1) The bytes that follow the template tag shall contain a valid length encoding (according to ASN.1 encoding rules). 2) The encoded length shall match the size of the given EF.DG12 object.

A.3.12.4 Test case SE_LDS_DG12_003

Test case-ID	SE_LDS_DG12_003
Purpose	This test checks the encoding of the SAI Reference String (Tag '82') present in EF.DG12.
Version	1.0
References	ISO/IEC 18013-3 ISO/IEC 8859-1
Profile	NMA
Preconditions	1) EF.DG12 has been retrieved from the IDL.

Test scenario	1) Search for the SAI Reference String (Tag '82') inside EF.DG12. 2) Check the encoded length of the SAI Reference String data element. 3) Check the length of the SAI Reference String data element. 4) Check the value of the SAI Reference String. 5) If the SAI Reference String starts with '00', check the value of the subsequent bytes of the SAI Reference String. 6) If the SAI Reference String starts with '01', check the value of the subsequent bytes of the SAI Reference String. 7) If the SAI Reference String starts with '01', check the value of the subsequent bytes of the SAI Reference String. 8) If the SAI Reference String starts with '01', check the value of the subsequent bytes of the SAI Reference String.
Expected results	1) Tag '82' shall be present. 2) The bytes that follow the Tag '82' shall contain a valid length encoding (according to ASN.1 encoding rules). 3) The encoded length shall match the size of the SAI Reference String data element. 4) The first byte of the SAI Reference String shall be '00' or '01'. 5) The subsequent bytes of the SAI Reference String shall be encoded in accordance with ISO/IEC 8859-1. 6) The subsequent bytes of the SAI Reference String shall be 2 BCD encoded bytes. 7) The second byte of the SAI Reference String shall refer to an existing Data Group in the IDL. 8) The third byte of the SAI Reference String shall refer to a field in an existing Data Group in the IDL that is available outside the ICC (i.e. DG1 Field 1..9, DG2 Field 1..7), or DG3 Field 1..4).

A.3.12.5 Test case SE_LDS_DG12_004

Test case-ID	SE_LDS_DG12_004
Purpose	This test checks the encoding of the SAI Input Method (Tag '81') present in EF.DG12.
Version	1.2
References	ISO/IEC 18013-3
Profile	NMA
Preconditions	1) EF.DG12 has been retrieved from the IDL.

Test scenario	1) Search for the SAI Input Method (Tag '81') inside EF.DG12. 2) Check the encoded length of the SAI Input Method data element, if present. 3) Check the length of the SAI Input Method data element. 4) Check the value of the SAI Input Method. 5) Check the value of the SAI Input Method. 6) If the SAI Input Method starts with '02', check the presence of byte 2 of the SAI Input Method. 7) Check the value of byte 2 of the SAI Input Method. 8) Check the value of byte 3 of the SAI Input Method, if present. 9) Check the value of the bytes 4 - 7 of the SAI Input Method, if present. 10) Check the consistency of the bytes 4 and 6 of the SAI Input Method, if present. 11) Check the consistency of the bytes 5 and 7 of the SAI Input Method, if present.
Expected results	1) Tag '81' may be present and shall not occur more than once. 2) The encoded length shall be '01', '02', or '07'. 3) The encoded length shall match the size of the SAI Input Method data element. 4) The first nibble of byte 1 of the SAI Input Method shall be '0', '1' or '2' or '4'. 5) The second nibble of byte 1 of the SAI Input Method shall be '0', '1' or '2'. 6) Byte 2 of the SAI Input Method shall be present. 7) Byte 2 of the SAI Input Method shall have one of the following values : '00', '01', '02', '03', 'FE', or 'FF'. 8) Byte 3 of the SAI Input Method shall have the value '00' or '01'. 9) Byte 4 - 7 of the SAI Input Method shall be BCD encoded. 10) Byte 4 of the SAI Input Method shall be smaller than byte 6 of the SAI Input Method. 11) Byte 7 of the SAI Input Method shall be smaller than byte 5 of the SAI Input Method.

A.3.13 Test unit SE_LDS_DG13 — Tests for EF.DG13

Test unit-ID	SE_LDS_DG13 (Standard Encoding — Data Group 13)
Purpose	The test cases in this test unit verify the structure and contents of the IDL LDS Data Group 13.
References	ISO/IEC 18013-2 ISO/IEC 18013-3 [TR-ICAO Part 3]